VMware vSphereを使用したRBAC

ONTAP tools for VMware vSphere 10

NetApp
August 25, 2025

This PDF was generated from https://docs.netapp.com/ja-jp/ontap-tools-vmware-vsphere-10/concepts/rbac-vcenter-environment.html on August 25, 2025. Always check docs.netapp.com for the latest.

目次

VMware vSphereを使用したRBAC . . . 1
vCenter Server RBAC環境とONTAP Tools for VMware vSphere 10 . . . 1
vCenter Serverアクセス許可の図 . . . 1
vCenter Serverアクセス許可のコンポーネント . . . 2
vCenter Server RBACとONTAP Tools for VMware vSphere 10の使用 . . . 2
vCenterのロールと管理者アカウント . . . 2
vSphereオブジェクト階層 . . . 3
ONTAP Tools for VMware vSphere 10に含まれるロール . . . 3
vSphereオブジェクトとONTAPストレージのバックエンド . . . 3
vCenter Server RBACノシヨウ . . . 3

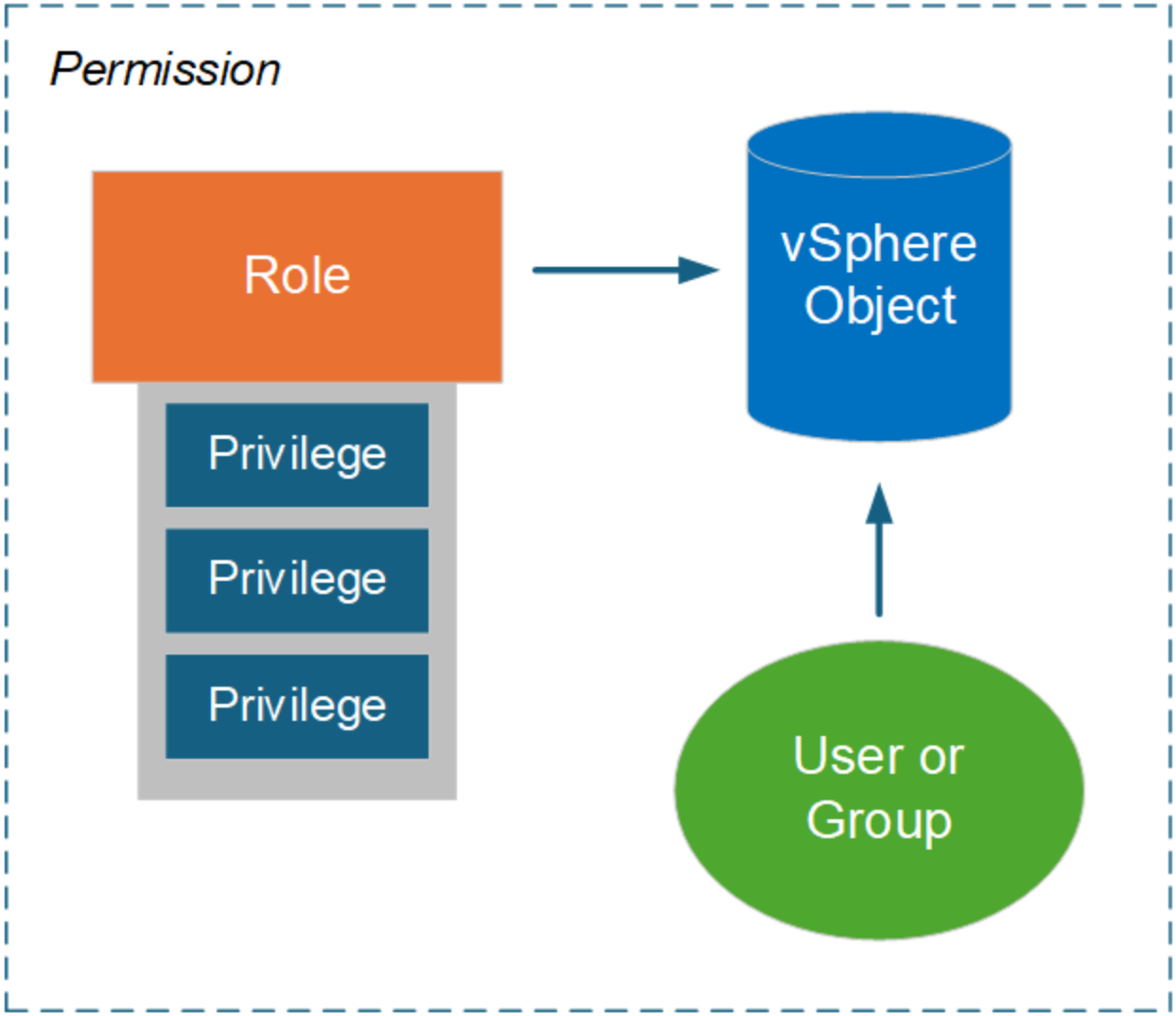
VMware vSphereを使用したRBAC

vCenter Server RBAC環境とONTAP Tools for VMware vSphere 10

VMware vCenter ServerにはRBAC機能が用意されており、vSphereオブジェクトへのアクセスを制御できます。これは、vCenterの一元化された認証および許可セキュリティサービスの重要な部分です。

vCenter Serverアクセス許可の図

アクセス許可は、vCenter Server環境でアクセス制御を適用するための基盤です。これは、アクセス許可の定義に含まれるユーザまたはグループを含むvSphereオブジェクトに適用されます。次の図に、vCenterアクセス許可の概要を示します。



vCenter Serverアクセス許可のコンポーネント

vCenter Serverアクセス許可は、アクセス許可の作成時にバインドされる複数のコンポーネントで構成されるパッケージです。

vSphere オブジェクト

アクセス許可はvSphereオブジェクトに関連付けられます。vCenter Server、ESXiホスト、仮想マシン、データストア、データセンター、フォルダなどがあります。vCenter Serverは、オブジェクトに割り当てられた権限に基づいて、各ユーザまたはグループがそのオブジェクトに対して実行できる操作またはタスクを決定します。ONTAP tools for VMware vSphereに固有のタスクについては、すべてのアクセス許可がvCenter Serverのルートフォルダレベルまたはルートフォルダレベルで割り当てられ、検証されます。詳細については、を参照してください "vCenter ServerでRBACを使用する" 。

Privilegesとロール

ONTAP Tools for VMware vSphere 10で使用されるvSphere Privilegesには、2つのタイプがあります。この環境でのRBACの使用を簡易化するために、ONTAP toolsには、必要なネイティブおよびカスタムのPrivilegesを含むロールが用意されています。Privilegesには以下が含まれます。

- vCenter Server 標準の権限

  これはvCenter Serverが提供するPrivilegesです。

- ONTAP tools固有の権限

  これらは、ONTAP Tools for VMware vSphereに固有のカスタムPrivilegesです。

ユーザとグループ

Active Directory またはローカルの vCenter Server インスタンスを使用して、ユーザーとグループを定義できます。ロールと組み合わせることで、vSphere オブジェクト階層内のオブジェクトに対する権限を作成できます。この権限は、関連付けられたロールの権限に基づいてアクセスを許可します。ロールはユーザーに直接個別に割り当てられるのではなく、ユーザーとグループは、vCenter Server のより広範な権限の一部として、ロール権限を通じてオブジェクトへのアクセスを取得します。

vCenter Server RBACとONTAP Tools for VMware vSphere 10の使用

ONTAP Tools for VMware vSphere 10 RBACのvCenter Serverへの実装については、本番環境で使用する前に考慮する必要があります。

vCenterのロールと管理者アカウント

カスタムのvCenter Serverロールを定義して使用する必要があるのは、vSphereオブジェクトおよび関連する管理タスクへのアクセスを制限する場合のみです。アクセスを制限する必要がない場合は、代わりに管理者アカウントを使用できます。各管理者アカウントは、オブジェクト階層の最上位レベルにある管理者ロールで定義されます。これにより、ONTAP tools for VMware vSphere 10によって追加されたvSphereオブジェクトを含む、vSphereオブジェクトへのフルアクセスが提供されます。

vSphereオブジェクト階層

vSphereオブジェクトインベントリは階層構造になっています。たとえば、次のように階層を下に移動できます。

```
vCenter Server→→→→ Datacenter Cluster ESXi host Virtual Machine
```

vSphereオブジェクト階層ではすべての権限が検証されますが、VAAIプラグインの処理はターゲットESXiホストに対して検証されます。

ONTAP Tools for VMware vSphere 10に含まれるロール

vCenter Server RBACの使用を簡易化するために、ONTAP Tools for VMware vSphereには、さまざまな管理タスクに合わせてカスタマイズされた事前定義されたロールが用意されています。

> 必要に応じて、新しいカスタムロールを作成できます。この場合は、既存のONTAP toolsロールのいずれかをクローニングし、必要に応じて編集する必要があります。設定を変更したら、影響を受けるvSphere Clientユーザがログアウトしてから再度ログインし、変更をアクティブ化する必要があります。

ONTAP tools for VMware vSphereのロールを表示するには、vSphere Clientの上部にある*を選択し、[管理]をクリックしてから、左側の[ロール]*をクリックします。以下に説明する3つの事前定義されたロールがあります。

VMware vSphere管理者向けNetApp ONTAPツール

VMware vSphere管理者タスク用のコアONTAPツールを実行するために必要なvCenter Server PrivilegesおよびONTAPツール固有のPrivilegesをすべて提供します。

NetApp ONTAP Tools for VMware vSphere読み取り専用

ONTAP toolsへの読み取り専用アクセスを許可します。アクセスが制御されたONTAP tools for VMware vSphereアクションを実行することはできません。

NetApp ONTAP Tools for VMware vSphereプロビジョニング

ストレージのプロビジョニングに必要なvCenter Server標準の権限とONTAP tools固有の権限が含まれています。次のタスクを実行できます。

- 新しいデータストアを作成する
- データストアを管理します

vSphereオブジェクトとONTAPストレージのバックエンド

2つのRBAC環境が連携して動作します。vSphere Clientインターフェイスでタスクを実行する場合は、まずvCenter Serverに定義されているONTAP toolsのロールがチェックされます。処理がvSphereで許可されている場合は、ONTAPロールPrivilegesが検証されます。2番目の手順は、ストレージバックエンドの作成および設定時にユーザに割り当てられたONTAPロールに基づいて実行します。

vCenter Server RBACノシヨウ

vCenter ServerのPrivilegesとアクセス許可を使用する際に考慮すべき点がいくつかあります。

必要な権限

ONTAP tools for VMware vSphere 10のユーザインターフェイスにアクセスするには、ONTAP tools固有の_view_privilegeが必要です。この権限がない状態でvSphereにサインインし、NetAppアイコンをクリックすると、ONTAP tools for VMware vSphereにエラーメッセージが表示され、ユーザインターフェイスにアクセスできません。

vSphereオブジェクト階層の割り当てレベルによって、ユーザインターフェイスのどの部分にアクセスできるかが決まります。ルートオブジェクトにView権限を割り当てると、NetAppアイコンをクリックしてONTAP tools for VMware vSphereにアクセスできるようになります。

代わりに、別の下位のvSphereオブジェクトレベルにView権限を割り当てることができます。ただし、これにより、アクセスして使用できるONTAP Tools for VMware vSphereメニューが制限されます。

権限を割り当てます

vSphereのオブジェクトおよびタスクへのアクセスを制限する場合は、vCenter Serverアクセス許可を使用する必要があります。vSphereオブジェクト階層で権限を割り当てる場所によって、ユーザが実行できるONTAP tools for VMware vSphere 10タスクが決まります。

> アクセスをより制限的に定義する必要がないかぎり、ルートオブジェクトレベルまたはルートフォルダレベルで権限を割り当てることをお勧めします。

ONTAP tools for VMware vSphere 10で使用できる権限は、ストレージシステムなどのvSphere以外のカスタムオブジェクトに適用されます。割り当て可能なvSphereオブジェクトがないため、可能であればこれらのアクセス許可をONTAP tools for VMware vSphereルートオブジェクトに割り当てる必要があります。たとえば、ONTAP tools for VMware vSphereの「Add/Modify/Remove storage systems」権限を含むすべてのアクセス許可は、ルートオブジェクトレベルに割り当てる必要があります。

オブジェクト階層の上位レベルでアクセス許可を定義する場合は、アクセス許可が子オブジェクトに継承されるように設定できます。必要に応じて、親から継承したアクセス許可を上書きする追加のアクセス許可を子オブジェクトに割り当てることができます。

権限はいつでも変更できます。アクセス許可に含まれるPrivilegesを変更した場合、アクセス許可に関連付けられているユーザが変更を有効にするには、vSphereからログアウトしてログインし直す必要があります。

著作権に関する情報

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。